



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

AB

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,043	10/25/2001	Huayan A. Wang	1190	8635
7590	01/31/2006		EXAMINER	
Oleg F. Kaplun, Esq FAY KAPLUN & MARCIN LLP 150 Broadway Suite 702 New York, NY 10038			KIM, JUNG W	
			ART UNIT	PAPER NUMBER
			2132	
			DATE MAILED: 01/31/2006	

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/026,043	WANG ET AL.	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 22 December 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-21 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 25 October 2001 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____

DETAILED ACTION

1. This Office action is in response to the amendment filed on December 22, 2005.
2. Claims 1-21 are pending.
3. Claims 1, 4 and 10 are amended.
4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

5. The 112/2nd paragraph rejection to claim 4 is withdrawn as the amendment overcomes the 112/2nd paragraph rejection.

Response to Arguments

6. Applicant's arguments with respect to the 102(e) rejection(s) of claim(s) 1-5, 10 and 14-16 under as being anticipated by Leung, the 102(e) rejections of claims 1-3, 6, 10-12, 14 and 16-18 as being anticipated by Singhal, the 103(a) rejections of claims 7, 8, 9, 13 and 15 as being unpatentable over Singhal in view of Vij or Singhal '761, and the 103 rejections of claims 19-21 as being unpatentable over Singhal in view of Singhal '761 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of the combined teachings of Singhal, Leung, Vij and/or US Patent Application no. 2002/0174335 Zhang et al. as outlined below.

Claim Rejections - 35 USC § 103

7. Claims 1-3, 6, 10-12, 14 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Singhal et al. USPN 6,851,050 (hereinafter Singhal '050) in view of Leung USPN 6,760,444. (hereinafter Leung)

8. As per claim 1, Singhal '050 discloses a method for authenticating a roaming device with a network, comprising the steps of:

- a. generating, by an authentication server of the network, authentication data associated with the roaming device (col. 18:45-46);
- b. sending, by the authentication server, the authentication data to access points of the network, the access points being connected to the authentication server(18:61-64); and
- c. when the roaming device roams to a particular access point of the access points, using the authentication data to authenticate the roaming device at the particular access point. (18:65-67)

Singhal '050 does not disclose authenticating the roaming device locally at the particular access point. Leung discloses a method and apparatus for authenticating a mobile node with a Home Agent, wherein the security association to authenticate the mobile node is retrieved from the authentication server by the Home Agent. (7:23-50) In order to reduce the number of authentication requests to the authentication server for the mobile node, the security association is temporarily stored in the Home Agent. (7:50-

Art Unit: 2132

67) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Leung with the invention of Singhal '050 such that the authentication data is stored at the access points of the network to locally authenticate the roaming device at a particular access point. One would be motivated to do so to reduce traffic between the authentication server and the access points as taught by Leung. (7:64-66) The aforementioned covers the limitation of claim 1.

9. As per claim 2, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (supra) In addition, the method further comprising the step of storing the authentication data in a memory arrangement of each of the access points. (Singhal '050, col. 18:64, 19:15-26)

10. As per claim 3, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (supra) In addition, the sending step includes the substeps of: encrypting the authentication data to selected access points of the access points. (Singhal '050, col. 18:64)

11. As per claim 6, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (supra) In addition, the method further comprising the preliminary steps of determining if the particular access point has authentication data associated with the roaming device; if the determination is positive, proceed to the step of using the authentication data to

locally authenticate the roaming device at the particular access point; and if the determination is negative, proceed to the step of generating, by an authentication server of the network, authentication data associated with the roaming device. (Singhal '050, fig. 15)

12. As per claim 10, Singhal '050 discloses a method for authenticating a roaming device with a network, comprising the steps of:

- d. connecting the roaming device with an authentication server upon a contact of the roaming device with a first access point of the network (18:40-45);
- e. authenticating the roaming device with the authentication server (18:45);
- f. generating authentication data for the roaming device(18:49-65);
- g. distributing, by the authentication server, the authentication data to the first access point and a second access point of the network (18:60-65); and
- h. authenticating the roaming device upon a contact with the second access point using the distributed authentication data. (18:65-67)

Singhal '050 does not disclose authenticating the roaming device locally at the particular access point. Leung discloses a method and apparatus for authenticating a mobile node with a Home Agent, wherein the security association to authenticate the mobile node is retrieved from the authentication server by the Home Agent. (7:23-50) In order to reduce the number of authentication requests to the authentication server for the mobile node, the security association is temporarily stored in the Home Agent. (7:50-67) Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made to combine the teaching of Leung with the invention of Singhal '050 such that the authentication data is stored at the access points of the network to locally authenticate the roaming device at a particular access point. One would be motivated to do so to reduce traffic between the authentication server and the access points.

(Leung, 7:64-66) The aforementioned covers the limitation of claim 10.

13. As per claim 11, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (supra) In addition, the method further comprising the step of authenticating the roaming device with the authentication server if the local authentication of the roaming device fails.

(Singhal '050, 18:40-45; 19:20-23)

14. As per claim 12, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. In addition, the distributing step further includes the substep of distributing an encrypted session key to the first and second access points. (Singhal '050, 18:61-64)

15. As per claim 14, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (supra) In addition, the method further comprising the steps of establishing a shared secret encryption between the authentication server and the first and second access points.

(Singhal '050, 18:64)

16. As per claim 16, Singhal '050 discloses a system for authenticating a roaming device with a network, comprising:

- i. an authentication server connected to the network (fig. 14); and
- j. first and second access points connected to the authentication server, the first and second access points being capable of communicating with the roaming device, each of the first and second access points including a memory arrangement capable of storing authentication data corresponding to the roaming device (18:66; 19:20-26),
- k. wherein the authentication server sends the authentication data to the first and second access points upon an initial authentication procedure of the roaming device with the first access point (18:61-67), and
- l. wherein the second access point authenticates the roaming device upon a contact of the roaming device with the second access point. (18:65-67)

Singhal '050 does not disclose authenticating the roaming device locally at the particular access point. Leung discloses a method and apparatus for authenticating a mobile node with a Home Agent, wherein the security association to authenticate the mobile node is retrieved from the authentication server by the Home Agent. (7:23-50) In order to reduce the number of authentication requests to the authentication server for the mobile node, the security association is temporarily stored in the Home Agent. (7:50-67) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Leung with the invention of Singhal '050

such that the authentication data is stored at the access points of the network to locally authenticate the roaming device at a particular access point. One would be motivated to do so to reduce traffic between the authentication server and the access points as taught by Leung. (7:64-66) The aforementioned covers the limitation of claim 16.

17. As per claim 17, the rejection of claim 16 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (supra) In addition, the second access point authenticates the roaming device with the authentication server if the authentication data is not found in the memory arrangement of the second access point. (Singhal '050, fig. 15)

18. As per claim 18, the rejection of claim 16 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (supra) In addition, the second access points authenticates the roaming device with the authentication server if the local authentication of the roaming device at the second access point fails. (Singhal '050, 19:20-26)

19. Claims 4 and 5 are rejected under 35 USC 103(a) as being unpatentable over Singhal '050 in view of Leung, and further in view of Ablay et al. USPN 5,408,683. (hereinafter Ablay)

20. As per claim 4, the rejection of claim 3 under 35 USC 103(a) as being unpatentable over Singhal '050 in view of Leung is incorporated herein. (supra) Singhal '050 does not disclose using prediction algorithms to anticipate where the roaming device will roam to determine to which access points to send the encrypted authentication data. Ablay discloses a method of tracking subscribers in a networked radio communications system having a plurality of trunked communication networks using location information of the subscribers to anticipate a roaming unit's location to reduce the number of registrations and de-registrations of the roaming unit. (col. 5:19-60; 6:26-57) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Ablay with the invention of Singhal '050 and Leung to use prediction algorithms to anticipate where the roaming device will roam to determine to which access points to send the encrypted authentication data. One would be motivated to do so to reduce the transmission overhead in keeping track of roaming subscribers. (Ablay, 3:30-37) The aforementioned cover the limitations of claim 4.

21. As per claim 5, the rejection of claim 4 under 35 USC 103(a) as being unpatentable over Singhal '050 in view of Leung is incorporated herein. (supra) In addition, in view of Ablay, the limitation of sending the encrypted authentication data to all the access points is an obvious enhancement in view of the teaching of Ablay that a mobile unit's registration is maintained at all access points in the anticipated probable

locations of the mobile unit. (Ablay, col. 5:19-26) The aforementioned cover the limitations of claim 5.

22. Claims 7, 8 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Singhal '050 in view of Leung, and further in view of Vij et al. USPN 6,452,910. (hereinafter Vij '910)

23. As per claim 7, the rejection of claim 6 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (supra) In addition, the step of using the authentication data to locally authenticate the roaming device further comprises reassociating the roaming device with the particular access point of the access points by providing identification information. (fig. 15, reference nos. 1510 and 1520) However, Singhal '050 only discloses that the roaming device provides identification, and does not disclose that an exchange occurs between the roaming device and access points to reassociate. Vij '910 discloses a management means for wireless access points wherein wireless devices are mutually authenticated with access points utilizing a common link key to verify that the wireless device is authorized to access the access point, and to ensure that the access point is the intended receiver. (col. 11:1-7) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reassociating to include a mutual authentication between the roaming device and the access point, since it is desirous to verify that the

participants belong to the same local network. (Vij, *ibid*) The aforementioned cover the limitations of claim 7.

24. As per claim 8, the rejection of claim 7 under 35 U.S.C. 103(a) is incorporated herein. (*supra*) In addition, the reassociating step further includes the substeps of:

m. searching a memory arrangement of the particular access point for the authentication data associated with the roaming device; and if the authentication data is found, performing a mutual authentication procedure between the roaming device and the particular access point. (Singhal '050; Willins, paragraph 17)

25. As per claim 13, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (*supra*) In addition, Singhal discloses the locally authenticating step further includes the substeps of:

n. providing identification data by the roaming device to the second access point; and correlating the identification data with the distributed authentication data. (18:40-42 and 65-67)

26. However, Singhal '050 only discloses that the roaming device provides identification, and does not disclose exchanging identification between the roaming device and access points to reassociate. Vij discloses a management means for wireless access points wherein wireless devices are mutually authenticated with access

points using a common link key to verify that the wireless device is authorized to access the access point, and to ensure that the access point is the intended receiver. (col. 11:1-7)

7) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reassociating to include a mutual authentication between the roaming device and the access point, since it is desirous to verify that the participants of a transmission belong to the same local network. (Vij, *ibid*) The aforementioned cover the limitations of claim 13.

27. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Singhal '050.

28. As per claim 9, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (*supra*) In addition, the generating step further includes the steps of:

- o. receiving an authentication request from the roaming device; determining that the roaming device can be granted access to network services; and generating an encrypted session key associated with the roaming device in the authentication server. (18:40-64)

29. Singhal '050 does not expressly teach the authentication request is encrypted. However, it is notoriously well known that authentication data transmitted in the clear is susceptible to sniffing attacks. To prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver.

Art Unit: 2132

For example, in the RADIUS protocol, a password transmitted from a client to an authentication server is hidden using a shared secret. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the authentication data to be transmitted securely to prevent the data from being stolen. The aforementioned cover the limitations of claim 9.

30. Claims 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Singhal '050 in view of Leung, and further in view of Zhang et al. US Patent Application no. 20020174335 (hereinafter Zhang); RFC 2138 is incorporated to illustrate inherent properties of the RADIUS protocol.

31. As per claim 15, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over by Singhal '050 in view of Leung is incorporated herein. (supra) Singhal '050 does not disclose the authentication server is a remote authentication dial-in user server. Zhang discloses an authentication procedure for mobile devices designed by Cisco wherein a roaming user is authenticated via an access point, and uses the RADIUS protocol to authenticate the user to the authentication server. (pg. 3, paragraphs 44-46) Further, the RADIUS protocol is the de-facto standard for remote authentication as known in the art. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the authentication server to be a RADIUS server, since it is desirous to implement protocols that have gained wide acceptance for reasons including, inter alia, standardization of design.

32. As per claim 19, Singhal '050 discloses a method for authenticating a roaming device with a network, comprising the steps of:

p. with an authentication server, receiving an authentication request from a roaming device; with the authentication server, generating a session key associated with the roaming device; sending the session key to an access point of the network, the session key being encrypted with a second shared code; and utilizing the session key to authenticate the roaming device at the access point, and to encrypt data exchanged between the roaming device and the access point. (col. 18:40-67)

33. Singhal '050 does not expressly disclose the authentication request received from the roaming device is encrypted with a first shared code. Zhang discloses an authentication procedure for mobile devices designed by Cisco wherein a roaming user is authenticated via an access point, and uses the RADIUS protocol to authenticate the user to an authentication server. Upon, authentication, an encrypted session key is delivered from the authentication server to the access point and the user (pg. 3, paragraphs 44-46; RFC 2138, pg. 4, last sentence, section 2, the password is encrypted using a method based on the RSA message digest algorithm MD5) Further, it is notoriously well known that authentication data transmitted in the clear is susceptible to sniffing attacks; to prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made

for the authentication data to be transmitted securely to prevent the data from being stolen. The aforementioned cover the limitations of claim 19.

34. As per claim 20, the rejection of claim 19 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the method further comprising the step of sending the encrypted session key to a further access point of the network to authenticate the roaming device at the further access point. (Singhal '050, col. 18:64)

35. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Singhal '050 in view of Zhang, and further in view of Quick, Jr. USPN 6,178,506 (hereinafter Quick '506).

36. As per claim 21, the rejection of claim 19 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Singhal '050 discloses the method further comprising the steps of:

- q. generating a first key of the session key to perform authentication of the roaming device at the access point (fig. 15, reference no. 1500); and
- r. generating a second key of the session key to encrypt data exchanges between the roaming device and the access point. (fig. 15, reference no. 1570a)

37. Singhal '050 does not expressly teach the first key as being different from the second key. Quick '506 discloses an authentication method wherein a first portion of a session key is used for authentication and a second portion of the session key is used

Art Unit: 2132

for encryption. Since, the session key is larger than the required byte size necessary for authentication, the portion not used for authentication is used for encryption. (col. 5:38-50) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first key generated from the session key to perform authentication and the second key generated from the session key to perform encryption to be different keys, since the protocols for authentication and encryption typically require different length keys. (Quick '506, 5:45-50) The aforementioned cover the limitations of claim 21.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

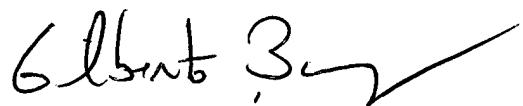
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

January 23, 2006



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100